# UN GROS REQUIN DE L'INTRUSION

*LE 12 DÉCEMBRE 2011* ***JEAN MARC MANACH***

**En partenariat avec WikiLeaks, OWNI révèle le fonctionnement de FinFisher, l'une de ces redoutables armes d'espionnage utilisées par les États. Description technique, mode d'emploi détaillé et résultats... inquiétants.**

L'opération **SpyFiles** initiée par WikiLeaks, et dont OWNI est partenaire, permet de révéler les noms des entreprises qui fournissent des chevaux de Troie aux services de police et de renseignement. C'est-à-dire ces systèmes introduits sur des disques durs, des fichiers, sur des messagerie et capables – pour les plus redoutables – d'espionner l'utilisateur en temps réel. Il s'agit de l'entreprise allemande **DigiTask**, qui a équipé les polices suisses et allemandes et qui, dans une plaquette de présentation commerciale qu'a pu consulter OWNI, présente sobrement son cheval de Troie comme un "*logiciel de police scientifique à distance*", mais également **ERA** (suisse), dont les systèmes espions étaient encore récemment utilisés en Syrie, **Hacking Team** (Italie), et **Gamma** (Grande-Bretagne), au travers de sa suite **FinFisher (™)**, dont OWNI a pu consulter l'intégralité du catalogue.

Remote Forensic Software

**2. What is Remote Forensic Software?**




– *Stealth software installed on computer of target to*
- overcome encryption
- handle nomadic targets
- monitor activity

for
- criminal investigations
- intelligence gathering





12

## Simple comme une clef USB

Le logo de FinFisher ? Un aileron de requin (*fin*, en anglais). Leader des "*techniques offensives de recueil d'information*", FinFisher, qui affirme ne travailler qu'avec des services de renseignement et forces de l'ordre, affiche clairement la couleur. Son portefeuille de produits propose une gamme complète d'outils d'espionnage informatique et de "*solutions d'écoute, de contrôle et d'infection à distance*" des ordinateurs à même de "*prendre le contrôle (et) d'infecter à distance les systèmes cibles*", afin de pouvoir espionner les messages reçus ou envoyés, d'accéder à toutes ses données, même et y compris si elles sont chiffrées.

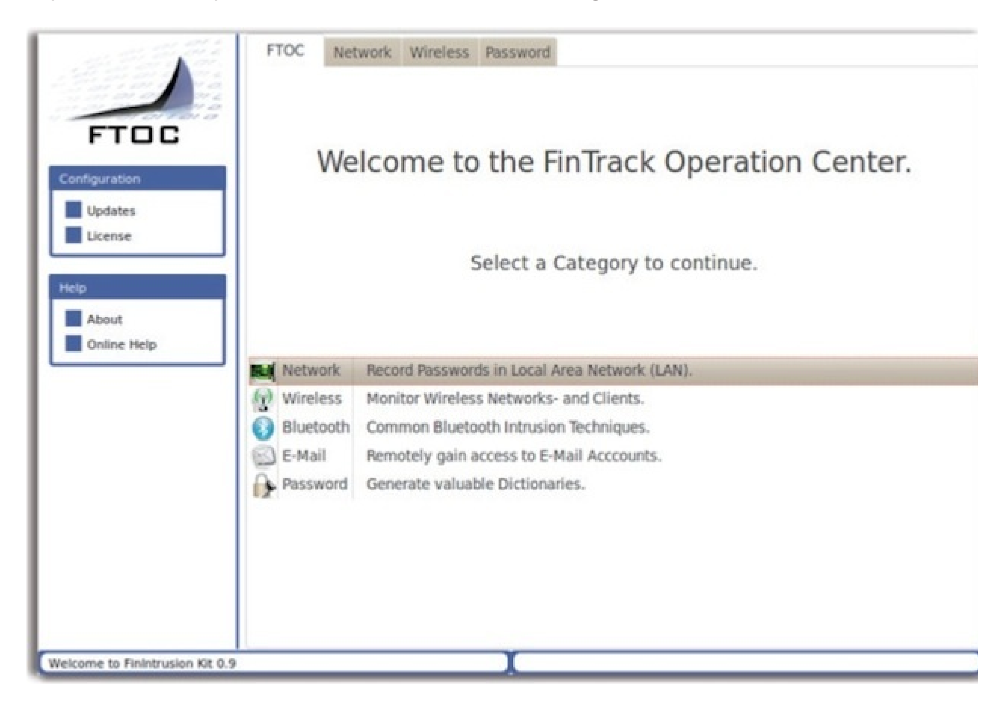
Son portfolio de présentation présente toute la gamme de solutions, qui n'ont rien à envier aux outils utilisés par les pirates informatiques, mais qui donnent la mesure de ce qu'il est possible de faire aujourd'hui. Dans une autre présentation de ses activités, datant de 2007, FinFisher se vantait ainsi d'"*utiliser et incorporer les techniques de hacking black hat (du nom donné aux hackers qui oeuvrent du côté obscur de la force, et en toute illégalité, NDLR) afin de permettre aux services de renseignement d'acquérir des informations qu'il serait très difficile d'obtenir légalement.*"




Vous avez la possibilité d'accéder physiquement à l'ordinateur de votre cible ? Insérez-y FinUSB, une petite clef USB créée tout spécialement pour extraire d'un ordinateur l'intégralité des identifiants et mots de passe qui s'y trouvent, les derniers fichiers ouverts ou modifiés, l'historique des sites visités, des communications instantanées, le contenu de la poubelle, etc., sans même que son propriétaire ne s'en aperçoive : il suffit en effet d'insérer la clef USB dans l'ordinateur, au prétexte de partager avec lui tel ou tel fichier, pour que le logiciel espion siphonne, de façon subreptice et sans se faire remarquer, l'intégralité des données.

La technique est aussi utilisée par des espions qui, dans des salons professionnels, ou dans les bureaux de ceux qu'ils veulent espionner, laissent traîner une clef USB, espérant que leur cible, curieuse, cherche à la lire… et donc infecte son ordinateur.

Vous n'avez pas d'accès physique à l'ordinateur à espionner ? Pas de problème : "*pensé et créé par des spécialistes travaillant depuis plus de 10 ans dans le domaine de l'intrusion*" pour casser les mécanismes utilisés pour sécuriser les réseaux sans-fil de type Wi-Fi (WEP ou **WPA1 & 2**), FinIntrusion Kit, permet de "*surveiller à distance webmail (Gmail, Yahoo…) et réseaux sociaux (Facebook, MySpace)*" utilisés pas la cible à espionner, ses blogs, forums, etc., et de récupérer ses identifiants et mots de passe, même et y compris si la cible utilise le protocole **SSL**, protocole de sécurisation des échanges sur Internet.




"*Cheval de Troie professionnel* " (sic) utilisé, "*depuis des années*", pour faciliter le placement sous surveillance des cibles qui se déplacent régulièrement, chiffrent leurs communications ou se connectent de façon anonyme, "***et qui résident dans des pays étrangers*** " (c'est FinFisher qui souligne), FinSpy vise de son côté à prendre le contrôle, à distance et de façon furtive, de tout ordinateur utilisant "*les principaux systèmes d'exploitation Windows, Mac et Linux*", et sans qu'aucun des 40 antivirus les plus utilisés ne soit capable de le reconnaitre, et donc de le bloquer.

Une fois installé, FinSpy peut espionner en "*live*" le ou les utilisateurs de l'ordinateur infecté (en activant, à leur insu, webcam et microphone), mais également le géolocaliser, en extraire toutes les données, intercepter les échanges de mail et autres conversations, et notamment les appels et transferts de fichiers effectués avec Skype (dont l'algorithme de chiffrement, propriétaire mais créé par des développeurs estoniens qui ont connu la Russie soviétique, a été conçu pour **sécuriser** les communications). Pour plus de furtivité, la

connexion, à distance, passe par des **proxies anonymiseur**s empêchant de remonter jusqu'aux ordinateurs des espions.

FinSpy existe aussi en version mobile, afin d'aider les autorités "*qui ne disposent pas de système d'interception téléphonique*" à espionner les communications (voix, SMS, MMS, mails) émanant de téléphones portables (BlackBerry, iPhone, Windows ou Android), même et y compris si elles sont chiffrées, et d'accéder aux données (contacts, agendas, photos, fichiers) qui y sont stockées, ou encore de les géolocaliser en temps réel.

## Contaminé en consultant un site

FinFly a de son côté été conçu pour installer, de façon subreptice, un cheval de Troie permettant le contrôle à distance de l'ordinateur de ces suspects qui ne cliquent pas sur les pièces jointes qui leur sont envoyées, et savent peu ou prou comment protéger leurs ordinateurs :

> ***Il est quasi-impossible d'infecter les ordinateurs des cibles particulièrement au fait des questions de sécurité informatique, dont le système d'exploitation est régulièrement mis à jour et qui ne comporte donc pas de faille de sécurité facilement exploitable.***

FinFlyUSB permet ainsi d'infecter un ordinateur par le simple fait d'y connecter une clef USB. FinFly LAN (pour Local Area Network, ou **réseau local**) propose de faire de même, mais sans accès physique aux ordinateurs à espionner, en s'infiltrant dans un réseau (câble ou Wi-Fi, et notamment dans ceux des cybercafés ou des hôtels). FinFly ISP (pour Internet Service Provider, ou fournisseur d'accès internet, FAI en français) procède de manière encore plus massive, mais en s'infiltrant au sein même des FAI, afin de pouvoir déployer leurs logiciels espions "*à l'échelle d'une nation* ".

Dans les deux cas, l'objectif est d'infecter, "*à la volée* ", les fichiers que des cibles seraient en train de télécharger, d'envoyer de fausses mises à jour de sécurité vérolées, ou encore de "*manipuler*" les pages web visitées pour y insérer le cheval de Troie, de sorte que la simple consultation d'une page web entraîne la contamination des ordinateurs de ceux qui la visite.

Pour cela, FinFisher a développé FinFly Web, qui permet de créer des pages web piégées dont la simple consultation entraîne l'infection des ordinateurs qui les consultent, et sans qu'ils ne s'en aperçoivent. FinFisher explique ainsi comment des "*cibles*" ont été espionnées en visitant un sites web créé tout spécialement pour attirer leur attention.

Le portfolio explique également qu'il est possible de faire croire à l'utilisateur à espionner qu'il doit télécharger un fichier (plug-in Flash ou RealPlayer, applet Java, etc.) dûment signé par une société bien connue du marché, "*par exemple Microsoft* ", laissant entendre, soit que ces compagnies collaborent avec FinFicher, soit qu'il a réussi à pirater leurs certificats de sécurité censés pourtant précisément garantir l'authenticité des fichiers téléchargés…

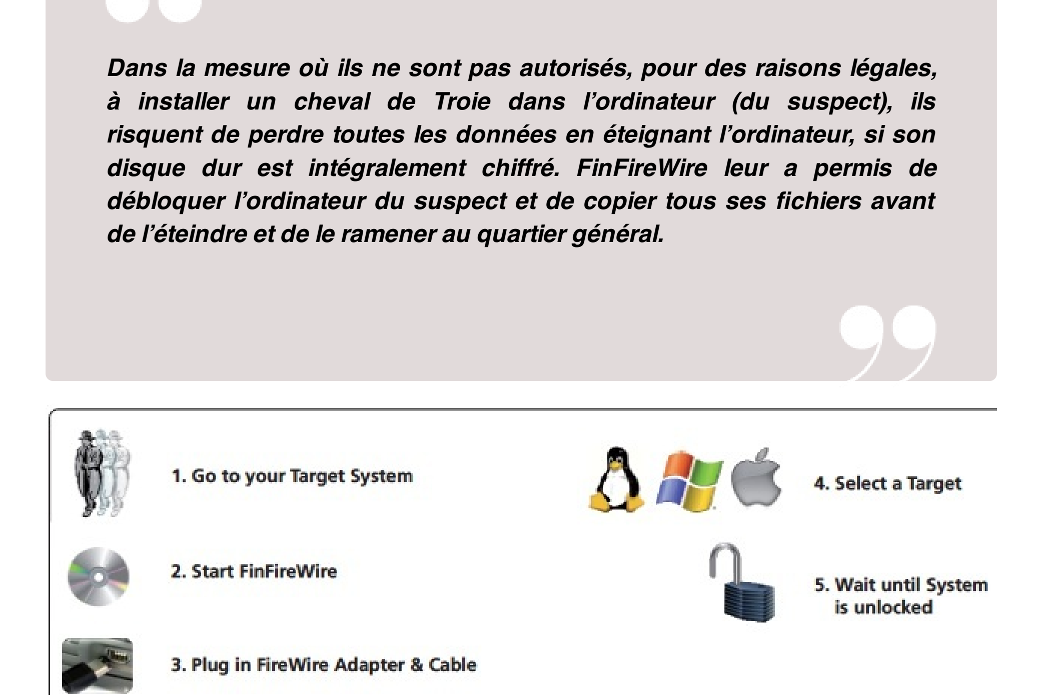
## Example: Java Applet (Internet Explorer, Firefox, Opera, Safari)

The website will prompt the Target to accept a Java plug-in that can be signed with any company name (e.g. "Microsoft Corporation")




FinFireWire permet, de son côté, d'accéder au contenu des ordinateurs (Windows, Mac et Linux) dont l'accès est protégé par un mot de passe, sans y laisser de trace. Le portfolio de FinFisher précise même qu'il permet également d'espionner sans contrôle judiciaire, évoquant le cas de policiers entrés dans l'appartement d'un suspect dont l'ordinateur, allumé, est protégé par un mot de passe :

> ***Dans la mesure où ils ne sont pas autorisés, pour des raisons légales, à installer un cheval de Troie dans l'ordinateur (du suspect), ils risquent de perdre toutes les données en éteignant l'ordinateur, si son disque dur est intégralement chiffré. FinFireWire leur a permis de débloquer l'ordinateur du suspect et de copier tous ses fichiers avant de l'éteindre et de le ramener au quartier général.***




## La "cyberguerre" à portée de clic

FinFisher propose également du "*FinTraining*" afin d'apprendre à ses clients à, "*par exemple*" : tracer des emails anonymes, accéder à distance à des comptes webmails, s'initier à l'intrusion sans-fil, "*attaquer les infrastructures critiques*", sniffer les identifiants, mots de passe et données circulant sur les réseaux, notamment les hotsposts Wi-Fi des cybercafés et des hôtels, intercepter les communications téléphoniques (VOIP et Dect), craquer les mots de passe… et autres techniques et méthodes de "*cyberguerre*".

**Fintraining 8601-01 : Basic Hacking Course (1 week) Intensive**

| | *Monday* | *Tuesday* | *Wednesday* | *Thursday* | *Friday* |
|---|---|---|---|---|---|
| *Week 1* | **FinFisher**<br>• FinFisher HQ<br>• FinFisher 1<br>• FinFisher 2<br>• FinFisher 3<br>**Toolset**<br>• FinFisher Hacking PC<br>• Equipment<br>• FinTrack<br>**Profiling**<br>Footprinting<br>• Search Engines<br>• Archives<br>• Target Websites<br>• "Who is" Records<br>• DNS Analysis<br>• First Contact | **Profiling**<br>Scanning<br>• Mapping<br>• Port scanning<br>• Service Fingerprinting<br>• OS Fingerprinting<br>• Analysis<br>Enumeration<br>• CGI<br>• NetBIOS<br>• SNMP<br>• RPC<br>• NFS<br>• Other | **Attacking**<br>Passwords<br>• Bypass<br>• Default<br>• Brute force<br>• Cracking<br>• Trusted<br>Web security<br>• Code Exposure<br>• Input Validation<br>• CGI<br>• XSS<br>• SQL Injection<br>• Other | **Attacking**<br>Exploits<br>• Overflows<br>• Format Strings<br>• Race Conditions<br>• Archives<br>• Exploiting<br>• Frameworks<br>• Fuzzer<br>Root-kits<br>• Backdoors<br>• Hiding<br>Log-cleaner<br>Network<br>• Sniffing<br>• Rerouting<br>• War-dialing | **Attacking**<br>Wireless LAN<br>• Discovery<br>• Encryption<br>• Advanced<br>• Hardware<br>Bluetooth<br>• Discovery<br>• Attacks<br>• Hardware<br>Advanced<br>• Custom Exploits |

**Gamma Group**, la société britannique à l'origine de FinFisher, se présente comme fournisseur de systèmes et technologies d'interception des télécommunications (internet, satellite -Thuraya, Inmarsat-, GSM, GPRS, SMS, etc.) à l'intention des agences gouvernementales et forces de l'ordre, à qui elle peut également vendre micro-espions et micro-caméras cachées de vidéosurveillance, camionnettes d'interception et outils de crochetage permettant d'ouvrir n'importe quelle porte…

Créée en 1990 et présente à Munich, Dubai, Johannesburg, Jakarta et Singapour, **Gamma** n'évoque nulle part le fait qu'elle se refuserait à vendre ces systèmes à des pays non démocratiques, ou connu faire peu de cas des droits de l'Homme.

En avril dernier, le *Wall Street Journal* **révélait** que des documents, découverts au siège de la "*division de la pénétration électronique* " (sic) de la police secrète égyptienne, démontraient que son logiciel espion avait bel et bien été utilisé pour espionner des militants politiques, les communications de l'un d'entre-eux ayant ainsi été espionnées. Il expliquait notamment l'importance d'utiliser Skype "*parce qu'il ne peut être pénétré par aucun dispositif de sécurité* " …

Basem Fathi, un activiste égyptien de 26 ans, a ainsi découvert que les services de sécurité égyptiens avaient été jusqu'à ficher sa vie amoureuse, et ses détours à la plage : "*je crois qu'ils collectionnaient tous les petits détails dont ils entendaient parler en nous écoutant, avant de l'enregistrer dans des fichiers*".

Un mémo "*Top Secret*" du ministère de l'Intérieur égyptien en date du 1er janvier 2011, que le *WSJ* a pu consulter, révèle que les autorités égyptiennes avait payé 388 604€ pour pouvoir tester le logiciel espion pendant cinq mois, et disposer du soutien de quatre employés du revendeur égyptien de Gamma, Modern Communication Systems. Ce qui leur a permis d'espionner de nombreux militants, allant jusqu'à la "*pénétration réussie de leurs réunions… quand bien même elles étaient chiffrées par Skype*".

Les Egyptiens n'étaient pas les seuls à être espionnés : les documents ont également **révélé** que les conversations de **Sherif Mansour**, représentant de l'ONG américaine Freedom House, venu en Egypte surveiller le bon déroulement des élections, avaient elles aussi été interceptées. Conscient de gêner les autorités, il avait précisément mis en place un "*protocole de sécurité consistant notamment à utiliser Skype aussi souvent que possible* ", au motif qu'il est plus sécurisé que les emails…

Interrogé par le *WSJ*, Mr Mansour se dit surpris : "*quand ils arrêtaient des blogueurs, ils les torturaient pour obtenir leurs mots de passe. Nous avions donc l'impression qu'ils ne pouvaient pas espionner nos conversations*".

A l'issue de la période d'essai, en décembre 2010, le ministère de l'Intérieur, satisfait, approuva l'achat du logiciel de Gamma. Le printemps arabe et la révolution égyptienne l'en a empêché.

Flash Player. To use iPaper (and lots of other stuff on the web) you need to **get the latest Flash player**.

Hello, you have an old version of Adobe Flash Player. To use iPaper (and lots of other stuff on the web) you need to **get the latest Flash player**.

FINFISHER™: GOVERNMENTAL IT INTRUSION
AND REMOTE MONITORING SOLUTIONS

WWW.GAMMAGROUP.COM

FINFISHER™
IT INTRUSION




Retrouvez **notre dossier** sur les *Spy Files* :

- **Mouchard sans frontière**

- **La carte d'un monde espionné**

Retrouvez nos articles sur **Amesys**.

Retrouvez tous **nos articles sur WikiLeaks** et ***La véritable histoire de WikiLeaks***, un ebook d'Olivier Tesquet paru chez OWNI Editions.

---

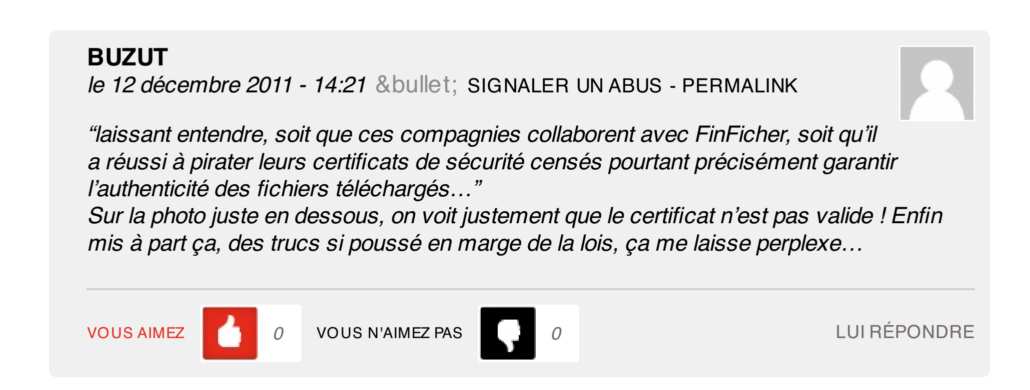
***@manhack*** *(sur Twitter),* ***jean.marc.manach*** *(sur Facebook &* ***Google+*** *aussi).*
*Vous pouvez également me contacter de façon sécurisée via* ***ma clef GPG/PGP*** *(ce qui, pour les non-initiés, n'est* ***pas très compliqué*** *). A défaut, et pour me contacter, de façon anonyme, et en toute confidentialité, vous pouvez aussi passer par* ***privacybox.de*** *(n'oubliez pas de me laisser une adresse email valide -****mais anonyme****- pour que je puisse vous répondre).*




*Pour plus d'explications sur ces questions de confidentialité et donc de sécurité informatique, voir notamment «* ***Gorge profonde: le mode d'emploi*** *» et «* ***Petit manuel de contre-espionnage informatique*** *».*

Retrouvez notre dossier sur le sujet :
**Une journée sous surveillance** et **Des chevaux de Troie dans nos démocraties**

Tous les articles OWNI/WikiLeaks **sont là**



**BUZUT**
*le 12 décembre 2011 - 14:21* • SIGNALER UN ABUS - PERMALINK

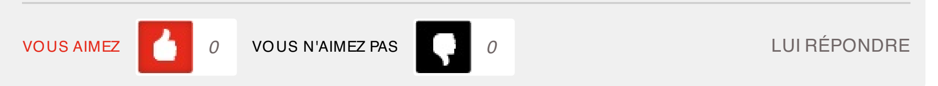
*"laissant entendre, soit que ces compagnies collaborent avec FinFicher, soit qu'il a réussi à pirater leurs certificats de sécurité censés pourtant précisément garantir l'authenticité des fichiers téléchargés…"*
*Sur la photo juste en dessous, on voit justement que le certificat n'est pas valide ! Enfin mis à part ça, des trucs si poussé en marge de la lois, ça me laisse perplexe…*

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

**STEPH**
*le 12 décembre 2011 - 18:19* • SIGNALER UN ABUS - PERMALINK

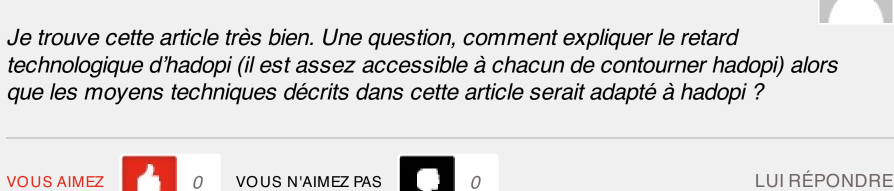
*@BUZUT: oué, enfin en même temps vu le nombre de sites tout à fait francs qui se traînent un certificat invalide (cf. coût prohibitif, toussa…), tout le monde a déjà passé outre à plusieurs reprises l'avertissement. De là, pas mal de gens peuvent avoir une baisse de vigilance face aux certificats non valides. Ballot ça.*

*Et sinon, l'ancien logo ressemble à celui de Wireshark, c'est juste une coïncidence ou ils ont mis des bouts de Wireshark dans FinFisher ?*



VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

**CYRIL**
*le 12 décembre 2011 - 23:02* • SIGNALER UN ABUS - PERMALINK



*Je trouve cette article très bien. Une question, comment expliquer le retard technologique d'hadopi (il est assez accessible à chacun de contourner hadopi) alors que les moyens techniques décrits dans cette article serait adapté à hadopi ?*

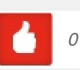
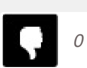
VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

**MICHEL**

*le 12 décembre 2011 - 23:33* • SIGNALER UN ABUS - PERMALINK

*Bonjour,*
*Je ne comprends pas trop qu'ils indiquent qu'ils peuvent signet une applet Java en faisant apparaître le nom d'une grande entreprise. C'est connu de toute personne ayant déjà eu à signer une applet Java. Il n'y a pas besoin d'avoir un bac + 8 en sécurité informatique : il suffit de répondre "Microsoft Corporation" à la création du certificat, quand l'outil demande l'organisation à laquelle vous appartenez…*
*Sinon, merci pour l'article, ça fait franchement peur…*

---

VOUS AIMEZ  *0* VOUS N'AIMEZ PAS  *0* LUI RÉPONDRE

**GOG**

*le 13 décembre 2011 - 8:54* • SIGNALER UN ABUS - PERMALINK

*Bonjour,*

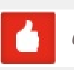
*Effectivement la signature des applets javas ne fonctionnent pas comme la certification type SSL et peuvent être signées absolument n'importe comment.*
*Très bon article au demeurant, le lien avec Wireshark (niveau logo) m'a apparu assez troublant également.*

*Difficile de faire face à ce genre d'intrusion, hélas, ToR ne suffit plus ! Ne reste plus qu'à créer son propre OS ou à se tourner vers l'option d'une virtualisation adéquate (ce qui est peu trivial pour un internaute moyen). Il serait intéressant de proposer des tutos à ce sujet.*

*Cdlmt,*

*GoG*

---

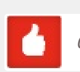
VOUS AIMEZ  *0* VOUS N'AIMEZ PAS  *0* LUI RÉPONDRE

**DARKMZ**

*le 13 décembre 2011 - 9:22* • SIGNALER UN ABUS - PERMALINK

*[mode Parano] Je pense toujours à ce genre de boite quand je clique – peut-être à tord – sur la MAJ automatique de mon FireFox 9 en phase Beta, en me disant que non, ce n'est pas possible, je le sais, je l'ai lu, personne ne pourrait venir s'intercaler entre le serveur de distro des MAJ Beta FFox et mon poste. Non, ce serait impossible. Ou bien ….. ;-) [/mode Parano]*

---

VOUS AIMEZ  *0* VOUS N'AIMEZ PAS  *0* LUI RÉPONDRE

**PHALKEN**

*le 14 décembre 2011 - 23:09* • SIGNALER UN ABUS - PERMALINK

*FinUSB : oki… sous Windows, télécharger une sam et la décrypter, je veux bien (j'ai un cd qui le fait en – 1-2 minutes, ou un petit script caché sur une clé USB qui permet juste de récupérer le fichier de pw). Par contre sous Linux, pour copier la base de données des pw, faut avoir le mot de passe root, sinon y a même pas d'accès en lecture, et après faut la décrypter en utilisant des attaque du type rainbow pour comparer les hash… et ça peut prendre bcp de temps (compter en années) même avec des gros calculateurs (mot de passe 12 caractère, chiffre, lettre, min/maj…).*

*Wep, wpa1, wpa2 : wep, je le fais avec mon téléphone en 2-3 min… wpa1, avec mon laptop en 5 à 10 min… par contre le wpa2,… mis à part quelques circonstances bien spécifiques, je vois pas comment ils s'y prennent..*

*Récupérer des identifiants et mots de passes à distance, même si utilisation du SSL apparemment en temps réel… là on passe carrément au stade divin de la chose…. tous les systèmes de confidentialité bancaire craqué dans le monde entier… si les banques et les mafias apprennent qu'une petite boîte en Allemagne peut faire ça… ça peut devenir sportif…*

*Non seulement ils maîtrisent mieux le cracking que la CIA, FBI et NSA réuni, mais ils ont en plus des techniques d'apprentissage qui feraient rougir de honte n'importe quels université / collège privé les plus vénérés au monde… heureusement, ils préviennent que c'est intensif, parce qu'enseigner les différentes techniques et type d'overflow, les backdoors, le sniffing de pc et le tri dans les logs de ces derniers, les techniques de*

*rerouting (genre attaque man on the middle j'imagine)… et je n'ai cité que 4 thème sur les 12 qu'il y a le jeudi… ben je dis chapeau… (et je ne parle même pas des autres journées…).*

*À mon avis soit*
*a) l'article est très mal écrit, manque de précision et/ou et exagère énoooormément.*
*b) soit la boîte se la raconte à mort pour impressionner.*

*Je ne parlerai pas des déchiffrage à la volée des BlackBerry, dont normalement seul les serveurs ont les clé de chiffrement (et, selon certaines rumeurs, p-e la NSA et les membre du programmes Echelon), et d'autres aberrations du même genre. Pour le reste… mouais… c'est du genre « j'infecte un pc avec un trojan et j'utilise wireshrak pour sniffer, et je suis la meilleure boîte d'intrusion au mooooooonde (le dire très fort à la proue d'un paquebot slalomant entre des iceberg).*

*Sérieusement, la moitié des choses me paraissent être du flan, le quart à la portée du premier script-kiddies venu, le reste, un peu de connaissance réseau et 2-3 soft du genre wireshark, aircrack-ng, qques tables pour les attaques sur les hash… ben rien de bien transcendantale à se mettre sous la dent. Bien sur, l'analyse des données*

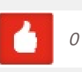
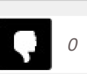
*P.S.*
*Apparemment, après avoir consulté les sites de ces société, tout est basé sur l'infection du pc par un trojan… effectivement, a partir de là, on peut tout avoir comme donnée… et ça n'importe quel scrip-kiddies de 15 ans peut le faire….*

*A bon entendeur…*

***Bon résumé de la situation; ne voulant pas perdre le lecteur non spécialiste de ces questions, j'ai du rester un peu "grand public", mais oui : ce que vend FinFisher, ce sont des trojans, avec cette particularité qu'ils ne seraient pas détecter par les AV,mais également la possibilité d'infecter un fichier à la volée, ce qui me semble un chouillas plus compliqué; quant à savoir jusqu'où ils sont capables de pénétrer des ordinateurs sous Mac OS ou GNU/Linux…***

*manhack*



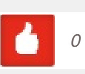
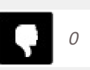
 0 VOUS N'AIMEZ PAS  0 LUI RÉPONDRE

**ACQUIER**
*le 15 décembre 2011 - 10:37* • SIGNALER UN ABUS - PERMALINK



*Je découvre ENFIN votre publication et votre adresse.*
*Je suis convaincu de pouvoir, ponctuellement, apporter de l'eau à votre moulin…*
*Je souhaite, bien évidemment m'informer et donc suivre vos informations et, éventuellement vous apporter mes commentaires.*
*Avec mes civilités citoyennes et irépressiblement humanistes;*
*Lou Destrabat*
*Le Désentravé ce 15/12/2011 .*



 0 VOUS N'AIMEZ PAS  0 LUI RÉPONDRE

**6 pings**

[Mondialisation sécuritaire] Un gros requin de l'intrusion » OWNI, News, Augmented | Club de l'Europe le 12 décembre 2011 - 14:35

*[...] L'opération SpyFiles initiée par WikiLeaks, et dont OWNI est partenaire, permet de révéler les noms des entreprises qui fournissent des chevaux de Troie aux services de police et de renseignement. C'est-à-dire ces systèmes introduits sur des disques durs, des fichiers, sur des messagerie et capables – pour les plus redoutables – d'espionner l'utilisateur en temps réel. Il s'agit de l'entreprise allemande DigiTask, qui a équipé les polices suisses et allemandes et qui, dans une plaquette de présentation commerciale qu'a pu consulter OWNI, présente sobrement son cheval de Troie comme un "logiciel de police scientifique à distance", mais également ERA (suisse), dont les systèmes espions étaient encore récemment utilisés en Syrie, Hacking Team (Italie), et Gamma (Grande-Bretagne), au travers de sa suite FinFisher (™), dont OWNI a pu consulter l'intégralité du catalogue. [...]*

Finisseur, un mouchard à tout faire au service de la police « Taditgeek le 12 décembre 2011 - 20:05

*[...] Jean-Marc Manach détaille chez Owni le contenu du catalogue de la société britannique Gamma, qui propose aux états sa suite de [...]*

FinFisher, un mouchard à tout faire au service de la police | UnderNews le 12 décembre 2011 - 20:26

*[...] Jean-Marc Manach détaille chez Owni le contenu du catalogue de la société britannique Gamma, qui propose aux états sa suite de [...]*

surveillance by stanjourdan - Pearltrees le 13 décembre 2011 - 11:30

*[...] "Cheval de Troie professionnel" (sic) utilisé, "depuis des années", pour faciliter le placement sous surveillance des cibles qui se déplacent régulièrement, chiffrent leurs communications ou se connectent de façon anonyme, "et qui résident dans des pays étrangers" (c'est FinFisher qui souligne), FinSpy vise de son côté à prendre le contrôle, à distance et de façon furtive, de tout ordinateur utilisant "les principaux systèmes d'exploitation Windows, Mac et Linux", et sans qu'aucun des 40 antivirus les plus utilisés ne soit capable de le reconnaitre, et donc de le bloquer. Un gros requin de l'intrusion » OWNI, News, Augmented [...]*

Fin Fisher | Computing bits le 14 janvier 2012 - 21:02

*[...] good example is finfisher, developed in the UK and offered worldwide. This entry was posted in Uncategorized. Bookmark the [...]*

FinSpy : le spyware britannique vendu à des régimes autoritaires ? | MecanoBlog le 4 septembre 2012 - 16:40

*[...] dernier, nous avions relayé un article d'Owni qui détaillait les redoutables promesses de la suite d'outils britannique FinFisher, [...]*